Student Exam No: _____

GANPAT UNIVERSITY
M. TECH. SEM.-I COMPUTER ENGINEERING/INFORMATION TECHNOLOGY
REGULAR EXAMINATION DECEMBER - 2016
3CE103/3IT103: CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours] **[Total Marks: 60**

Instructions:
1. Figures to the right indicate full marks.
2. Each section should be written in a separate answer book.
3. Be precise and to the point in your answer.

SECTION – I

Q.1 (a) Discuss about Step by Step Process of HMAC. (4)
(b) Discuss about Z_n, Z_n^* and Z_n+. (3)
(c) Find out the Multiplicative Inverse of 234 in Z_{4245}. Justify your answer. (3)

OR

Q.1 (a) Solve the following: (4)
1) $(-939)^{-1}$ mod 26
2) 19 ≡ ____ mod 101
(b) What is Euler"s phi Function (Ø (n))? Explain it. (3)
(c) How Rabin Crypto-System Works? Explain it in brief. (3)
Q.2 (a) Solve the Linear Congruence: $3x+2y \equiv 5 \pmod 7$ (5)
$4x+6y \equiv 4 \pmod 7$
(b) If Public key in RSA is (19, 3599) then find the corresponding private key. (5)

OR

Q.2 (a) Discuss about Pretty Good Privacy (E-Mail) Protocol in brief. (5)
(b) Encrypt the letter "D" using Knapsack Crypto System. Super increasing tuple b=[2,3,6,12,24,48] , Permutation Table [4,2,5,3,1,7,6], modulus n=98 and random integer r=5 is given. (note: ASCII value of „g" is 110011) (5)

Q.3 (a) Perform the Miller-Rabin Primality Test on following. (note: a=2) (6)
1) 123 2) 251
(b) Perform the Square Root Primality Test on following. (4)
1) 23 2) 29

SECTION – II

Q.4 (a) Encrypt the following message with vigenere cipher with key "abcdef" (5)
Plain text: "crypto is for cryptography".
(b) Define below mentioned attacks with real life example for each: (5)
1) DNS spoofing 2) Fabrication 3) DoS attack

OR

Q.4 (a) Discuss about Dynamic Packet filter with reference to Firewall. (5)

(b) Discuss about following: (5)

1) Repudiation 2) Snooping 3) Masquerade

Q.5 (a) Alice and Bob want to establish a secret key using the Diffie-Hellman key exchange protocol. Assuming the values as n = 17, g = 5, x = 4, y = 6, Find out the values of A, B and the secret key K1 and K2 (5)

(b) What are the differences between Confusion and Diffusion? (5)

OR

Q.5 (a) Explain Feistel Cipher Structure and its design features with diagram. (5)

(b) Discuss about Network Address Translation with Example. (5)

Q.6 (a) Show how the byte **13** is transformed to **7D** by subbyte routine in AES using $GF(2^8)$. (5)
Required constant matrix for calculation is given below.

Constant Matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Constant column matrix:

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

(b) Describe Rail fence cipher technique with example (take depth=3). (5)

----------End of Paper----------